IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EX PARTE DAVIS et al.

Application for Patent

Filed: July 22, 1999

Application No. 09/359,083

FOR:

INTERNET PAYMENT, AUTHENTICATION AND LOADING SYSTEM USING VIRTUAL SMART CARD

APPEAL BRIEF

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence is being transmitted to the U.S. Patent and Trademark Office, Central Facsimile Telephone number (571) 273-8300 on this day October 13, 2009 addressed to Examiner LIVERSEDGE, Jennifer L.
Signed: /Ann Lowe/
Ann Lowe

BEYER LAW GROUP LLP
Attorneys for Appellants

TABLE OF CONTENTS

		Page No.
I.	REAL PARTY IN INTEREST	1
II.	RELATED APPEALS AND INTERFERENCES	1
III.	STATUS OF CLAIMS	1
IV.	STATUS OF AMENDMENTS	1
V.	SUMMARY OF CLAIMED SUBJECT MATTER	1
VI.	GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	3
VII.	ARGUMENT	3
	A. *Davis* Does Not Disclose a Pseudo Card Reader Module	3
	B. *Davis* Does Not Disclose a Virtual Smart Card Database	5
	C. The Final Office Action Uses A Standard For Anticipating That Is Not Legally Correct	6
	D. Advisory Action Is Incorrect	8
VIII.	CONCLUSION	9
IX.	CLAIMS APPENDIX	10
X.	EVIDENCE APPENDIX	15
XI.	RELATED PROCEEDINGS APPENDIX	16

I. REAL PARTY IN INTEREST

The real party in interest is Visa International Service Association, a subsidiary of Visa Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or judicial proceedings known to the Appellants.

III. STATUS OF CLAIMS

Allowed claims:	None
Claims objected to:	None
Claims rejected:	1-8 and 34-49.

IV. STATUS OF AMENDMENTS

A response was filed by Applicant on July 1, 2009 in response to a Final Office action dated May 8, 2009. The amendments made in Applicant's response have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides an online purchase and load (OPAL) server that implements virtual smart cards. It provides software emulation of smart cards and smart card readers that operate with current Internet payment and loading systems. Advantageously, components of Internet payment and loading systems (such as the merchant server and payment server) and techniques for processing payment and load

transactions may remain the same when using the present invention. Use of the OPAL server of the present invention is transparent to merchants on the Internet. In one embodiment, a physical smart card and its associated card reader are emulated in software on a remotely-located OPAL server computer, thus obviating the need for physical smart cards and smart card readers. The existing client terminal acts as a pass-through device that is transparent to a user, a merchant server or a bank server.

Claim 1 recites an on-line purchase and load (OPAL) server computer (FIG. 2, 260; page 16, lines 24-33) for performing a purchase transaction over a network (FIG. 2, 202) using a virtual smart card (page 23, lines 10-13). One component of the server is a virtual smart card database (FIG. 4, 270) having multiple records, each record including a virtual card identifier and a balance amount that corresponds to a single virtual smart card (page 17, lines 34-35). A hardware security module (FIG. 4, 268) decrypts the balance, decreases the balance, and encrypts the decreased amount (page 18, line 34 to page 19, line 2). Another component of the server is a smart card emulator. FIG. 4, 266. This is a software module that receives smart card commands and processes them in conjunction with the virtual smart card database and the hardware security module. Page 20, lines 15-21. It is arranged to retrieve a record from the database and transmit the balance to the hardware security module and to store the encrypted decreased monetary balance in the record. Page 20, lines 15-21. Another component of the server is a pseudo card reader module. (FIG. 2, 204) This is also a software module that receives smart card commands related to the transaction over the network and relays the commands to the smart card emulator. Page 19, lines 30-33. In this manner, the OPAL server performs a transaction over the network using one of the records in the virtual smart card database. Page 16, lines 25-29.

Claim 41 also recites an OPAL server computer (FIG. 2, 260; page 16, lines 24-33) for performing a load transaction over a network (FIG. 2, 202; FIGS. 18A-18C) using a virtual smart card (page 23, lines 10-13). A component of the server is a virtual smart card database (FIG. 4, 270) having multiple records, each record including a virtual card identifier and a balance corresponding to a single virtual smart card (page 17, lines 34-35). A hardware security module (FIG. 4, 268) decrypts the balance, increases the

balance, and encrypts the increases amount (page 18, line 34 to page 19, line 2). Another component is a smart card emulator (FIG. 4, 266). This is a software component that receives smart card commands and processes the commands in conjunction with the virtual smart card database and the hardware security module (page 20, lines 15-21). It is arranged to retrieve a record from the database and transmit the balance to the hardware security module and to store the encrypted decreased monetary balance in the record. Page 20, lines 15-21. The smart card emulator is also configured to send a load request message to a load server (FIG. 18A, 878). The load request message indicates or contains a virtual smart card identifier and a load amount for a corresponding virtual smart card. The load amount indicates an amount of money to load onto the respective virtual smart card. Page 46, lines 25-31. Another component is a pseudo card reader module. (FIG. 2, 204). This is also a software module that receives smart card commands related to the transaction over the network and relays the commands to the smart card emulator. Page 19, lines 30-33. The OPAL server performs a transaction over the network using one of the records in the virtual smart card database. Page 16, lines 25-29.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejections presented for review are as follows:

The rejections of claims 1-8 and 34-49 under 35 U.S.C. §102 (e) as being anticipated by U.S. Patent No. 6,282,522 issued to *Davis et. al.*

VII. ARGUMENT

With respect to the ground above, the rejected claims are argued as a single group.

A. *Davis* Does Not Disclose a Pseudo Card Reader Module

The Final Office action, dated May 8, 2009, cites the *Davis* reference for disclosing a virtual smart card database, a smart card emulator, and a pseudo card reader,

all features recited in independent claims 1 and 41. However, *Davis* teaches using a physical smart card to make purchases using a payment system over the Internet. At issue is one sentence in *Davis* that states that the functionality of the physical smart card may be "implemented in software on a client terminal, that is, the card may be a 'virtual' card." [col. 11, lines 13-14]. This is the only instance where the term "virtual card" (or the term "virtual") is mentioned in *Davis*. The entire specification focuses solely on implementing a payment system using a physical smart card. It does not mention, let alone describe, how a virtual card may be enabled.

Instead, *Davis* describes various hardware components in an Internet payment system, such as a card reader, a payment server, a merchant server, among other components, none of which anticipate, under §102(e), a pseudo card reader module, virtual smart card database, or a smart card emulator. As discussed below, *Davis* is not a proper §102 reference because it is not enabling with respect to the claimed elements.

Davis clearly shows a physical smart card and a physical smart card reader, for example, as shown in Figures 4 and 16. In contrast, claims 1 and 41 require "a pseudo card reader module" rather than a physical card reader. A physical card reader is a tangible, physical device that reads a card. By contrast, the claimed pseudo card reader module is a software application that emulates functionality of a card reader. Support for a "pseudo card reader module" is found at various places in the present specification. For example, Figure 3, introduced at page 16, states "System 250 dispenses with the need for card reader 210 and smart card 5." At page 17, the second full paragraph provides that "server 260 emulates the physical smart card through the use of pseudo card reader module 264, smart card emulator 266, hardware security module 268 and card database 270." And, at the last paragraph on page 19, a pseudo card reader module "is a software module that performs the functionality of a physical card reader so that emulation of a smart card is transparent to client code module 224."

By contrast, *Davis* describes how its card reader must be physical, rather than a software module: a "card reader interface 24" includes software and hardware necessary

for communications with a card reader as shown in Figure 1. The card reader is described as having a contact interface in which signals from a microcontroller are routed to a number of metal contacts on the outside of the physical smart card which come in physical contact with similar contacts of a physical card reader. There is not a single mention of a pseudo card reader module in *Davis*, or any mention of a card reader being anything other than physical.

The Final Office action states that a pseudo card reader module is shown at column 7 of *Davis*, but this section clearly discloses only a physical card reader into which a physical card is inserted. Further, a citation to column 8 discloses only a physical security card. A reference to column 10 discloses only physical "stored value" cards and security cards that can only be inserted into a physical card reader. The final citation to column 11 likewise only discloses a physical security card. (*see* pg. 5 of Final Office action.) In sum, *Davis* describes contexts in which a cardholder "inserts his or her card into a card reader attached to a personal computer." (*see e.g.,* col. 7, lines 6-21). In other words the card reader of *Davis* must by physical.

For these reasons, it is respectfully submitted that *Davis* does not anticipate under §102 "a pseudo card reader module" as required by claims 1 and 41.

B. *Davis* Does Not Disclose a Virtual Smart Card Database

Claims 1 and 41 also recite "a virtual smart card database" in which each record stores a virtual card identifier and a balance that correspond to a single virtual smart card. An example of a virtual smart card database is shown in Figure 4. The Office action cites of sections of *Davis* to show a virtual smart card database, however all these citations fall short of anticipating the claimed element. The Office action cites column 10 of *Davis* as disclosing a virtual smart card database, but this section only discloses a payment server that manages a transaction database 223. Database 223 is not a database of records where each record corresponds to a virtual smart card. Another citation to column 11 only discloses a "processor" card (another name for a smart card) that has various functions. There is no mention of a database, let alone a virtual smart card database. A citation to

column 13 discloses a payment module that logs results and a reference to column 16 describes data from a smart card. None of these sections disclose a virtual smart card database where each record includes not only an identifier for a virtual card, but also a monetary balance for that card.

For these reasons, it is respectfully submitted that *Davis* does not anticipate a "virtual smart card database" as required by claims 1 and 41.

C. The Final Office Action Applies a Standard for Anticipation That Is Not Legally Correct When Concluding that a Smart Card Emulator is Shown

Claims 1 and 41 also recite "a smart card emulator." The second and third full paragraphs of page 20 clearly state that the smart card emulator is a software module and not a physical smart card.

The Office Action alleges that a smart card emulator is disclosed in column 7 of *Davis*, but this section discusses the cardholder inserting a physical card into a physical card reader. The Action also cites column 8, but this section describes a security card, which is another type of physical card. Column 10 also refers to a physical smart card. Finally, the reference to column 11 also clearly describes a security card as being a physical card which has an embedded microchip. Column 11, lines 10-14, disclose that "the functionality of stored value card 5 may be implemented in software on client terminal 204, that is, card 5 may be a 'virtual' card." But, this brief sentence falls short of providing an enabling disclosure of a virtual card and may not be relied upon for anticipation as explained below.

Applicant's reply on March 22, 2006 argued that the *Davis* reference does not teach or suggest "a smart card emulator" or "a pseudo card reader module" as required by claims 1 and 41 because there is no enabling description of these elements in *Davis*. In response, the Final Office Action stated that any disclosure in a reference may serve as anticipatory prior art (Final Office Action dated May 9, 2006, page 9, emphasis added). The Office Action stated: "...any disclosure serves as prior art and the disclosure as part

of the Davis description that other forms including a virtual card may also be one means of the invention (column 11, lines 10-14), establishes a virtual card as prior art within the disclosure of the invention and the description of functionality therein."

Applicant strenuously objects to the notion that "any disclosure" in a reference can serve as a basis for anticipation and asserts that the proper standard is that the disclosure in a reference must be enabling in order to be anticipatory.

Section 2121.01 of the MPEP states that "the standard test is whether a reference contains an enabling disclosure," and that "mere naming or description of the subject matter is insufficient, if it cannot be produced without undue experimentation."

In addition to the MPEP, case law further supports Applicant's position that the reference must be enabling to be anticipatory. In order to support a rejection under §102 or §103, a prior art reference must be enabling as conveyed by the United States Supreme Court:

> Patented inventions cannot be superseded by the mere introduction of a foreign publication of the kind, though of prior date, unless the description and drawings contain and exhibit a substantial representation of the patented improvement, in such full, clear, and exact terms as to enable any person skilled in the art or science to which it appertains, to make, construct, and practice the invention to the same practical extent as they would be enabled to do if the information was derived from a prior patent. Mere vague and general representations will not support such a defense, as the knowledge supposed to be derived from the publication must be sufficient to enable those skilled in the art or science to understand the nature and operation of the invention, and to carry it into practical use. Whatever may be the particular circumstances under which the publication takes place, the account published, to be of any effect to support such a defense, must be an account of a complete and operative invention capable of being put into practical operation.

(*Seymour v. Osbourne*, 78 U.S. 516, 555 (1870).

In the present situation, the requirement that a description be enabling is important because Applicant is asserting that the single passage that mentions a "virtual

card" in *Davis* is not enabling and thus cannot anticipate the element of "a smart card emulator" as required by claims 1 and 41. Recitation of this single phrase simply fails to enable a concept as complex as using software to emulate a smart card.

The claim rejections under 35 U.S.C. § 102 (e) as being anticipated by *Davis* cannot stand for at least the reasons discussed. The Examiner's reliance on *Davis* is misplaced, because the Examiner has failed to apply the correct legal standard for a reference to qualify as anticipatory.

For all these reasons, it is respectfully submitted that *Davis* does not anticipate "a smart card emulator" as required by claims 1 and 41.

D. Advisory Action Is Incorrect

Item 11 of the Advisory Action dated July 20, 2009 states that "... as the specification of Davis provides for the system and method as presented to be functional for either a physical or virtual card, the supporting systems such as databases and card readers anticipate either such systems for a physical or virtual card," referring to the sole mentioning of a "virtual card" in the present specification at column 11, lines 11-14.

Applicant understands this to mean that the Examiner believes that a system and method for implementing a virtual card is provided for in *Davis*, and that supporting systems, such as the physical smart card databases and physical card readers in *Davis*, anticipate systems for both a physical smart card and a virtual card. Applicant does not see how this can be. Systems and methods for providing a virtual smart card system are complex and very different from what is disclosed in *Davis* which, as discussed above, focuses solely on physical smart cards, and components and processes needed for implementing a physical smart card framework. It does not proffer, at any point in the specification, how this framework can be implemented using a virtual smart card, yet the Examiner would have us believe that the physical smart card system in *Davis* does just that by virtue of briefly mentioning the possibility of using software to implement a virtual smart card. For this and all the reasons explained above, the standard for

anticipation by a § 102 reference asserted by the Examiner in the Advisory Action is not correct.

VIII. CONCLUSION

In view of the foregoing, Appellants respectfully request that the Board reverse the Examiner's rejection of all pending claims. In addition, Appellants believe all claims now pending in this application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

Respectfully Submitted,

BEYER LAW GROUP LLP

Rupak Nag
Registration No. 37,493

IX. CLAIMS APPENDIX

CLAIMS ON APPEAL

1. An on-line purchase and load (OPAL) server computer for performing a purchase transaction over a network using a virtual smart card, said OPAL server computer comprising:

a virtual smart card database having a plurality of records, each record including a virtual smart card identifier and a monetary balance corresponding to a single virtual smart card;

a hardware security module arranged to decrypt said monetary balance, to decrease said monetary balance, and to encrypt said decreased monetary balance;

a smart card emulator that receives smart card commands from a pseudo card reader module and processes said commands in conjunction with said virtual smart card database and said hardware security module, said smart card emulator arranged to retrieve one of said records from said virtual smart card database, and to deliver said monetary balance to said hardware security module and to store said encrypted decreased monetary balance received from said hardware security module in said retrieved record; and

said pseudo card reader module that receives said smart card commands related to said purchase transaction over said network and relays said commands to said smart card emulator, whereby said OPAL server computer performs said purchase transaction over said network using one of said records in said virtual smart card database.

2. An OPAL server computer as recited in claim 1 wherein said virtual smart card database further includes purchase algorithm identifiers, wherein said hardware security module includes a plurality of purchase algorithms that are identified for use by one of said purchase algorithm identifiers, and wherein said hardware security module is arranged to decrypt said monetary balance using one of said purchase algorithms identified by one of said purchase algorithm identifiers.

3. An OPAL server computer as recited in claim 1 further comprising:

a user verification module that verifies a user accessing said OPAL server computer and generates a user identifier, said user identifier being suitable to identify one of said virtual smart card records in said virtual smart card database.

4. An OPAL server computer as recited in claim 1 wherein said smart card emulator and said pseudo card reader module are implemented as a single software module.

5. An OPAL server computer as recited in claim 1 wherein said network is an internet over which said OPAL server computer communicates with a merchant server and a payment server to transact said purchase transaction.

6. An OPAL server computer as recited in claim 1 wherein said network is an internet over which said OPAL server computer communicates with a bank server and a load server to load value onto said virtual smart card.

7. An OPAL server computer as recited in claim 1 wherein said network is an internet over which said OPAL server computer communicates with a web server and an authentication server to authenticate a user.

8. An OPAL server computer as recited in claim 1 wherein said OPAL server computer communicates over said network with a payment gateway for funding account authorization and clearing.

Claims 9-33 canceled.

34. An OPAL server computer as recited in claim 1 wherein said smart card emulator is suitable for returning said record to said virtual smart card database.

35. An OPAL server computer as recited in claim 1 wherein each record of the virtual smart card database also includes a funding account number wherein the funding account number identifies an account that contains a monetary amount that can be loaded onto a virtual smart card.

36. An OPAL server computer as recited in claim 1 wherein the OPAL server is further configured to receive a purchase request message from a client terminal, wherein the purchase request message indicates a good or service to be purchased by a user, a user identifier, and a user password.

37. An OPAL server computer as recited in claim 36 wherein the OPAL server is further configured to send a draw request message to a payment server, wherein the draw request message indicates an amount of money required to purchase the good or service and a merchant identifier.

38. An OPAL server computer as recited in claim 37 wherein the OPAL server computer is further configured to receive a debit command from the payment server, wherein the debit command indicates an amount of money to debit from a respective virtual smart card.

39. An OPAL server computer as recited in claim 38 wherein the smart card emulator is configured to debit itself in response to the debit command by the amount of money indicated in the debit command.

40. An OPAL server computer as recited in claim 38 wherein the OPAL server computer is further configured to send a debit response message to the client terminal, wherein the debit response message informs the user either that the amount of money has

been debited from the smart card emulator or that money has not been debited from the smart card emulator due to a lack of sufficient funds.

41. An on-line purchase and load (OPAL) server computer for performing a load transaction over a network using a virtual smart card, said OPAL server computer comprising:

a virtual smart card database having a plurality of records, each record including a virtual smart card identifier and a monetary balance corresponding to a single virtual smart card;

a hardware security module arranged to decrypt said monetary balance, to increase said monetary balance, and to encrypt said increased monetary balance;

a smart card emulator that receives smart card commands and processes said commands in conjunction with said virtual smart card database and said hardware security module, the smart card emulator also configured to send a load request message to a load server, wherein the load request message indicates a virtual smart card identifier and a load amount for a respective virtual smart card, the load amount indicating an amount of money to load onto the respective virtual smart card, said smart card emulator arranged to retrieve one of said records from said virtual smart card database and to deliver said monetary balance to said hardware security module and to store said encrypted increased monetary balance received from said hardware security module in said retrieved record; and

a pseudo card reader module that receives said smart card commands related to said load transaction over said network and relays said commands to said smart card emulator, whereby said OPAL server performs said load transaction over said network using one of said records in said virtual smart card database.

42. An OPAL server computer as recited in claim 41 wherein the OPAL server is configured to receive a load command from a load server wherein the amount of money indicated in the load request message is loaded onto the respective virtual smart card.

43. An OPAL server computer as recited in claim 42 wherein the smart card emulator is configured to send a load response message to a client terminal, wherein the load response message informs a user that the amount of money has been loaded onto the respective virtual smart card.

44. An OPAL server computer as recited in claim 1 further comprising:

a memory arranged to store said virtual smart card database, said smart card emulator, and said pseudo card reader module.

45. An OPAL server computer as recited in claim 1 wherein said hardware security module is a hardware device in said OPAL server computer.

46. An OPAL server computer as recited in claim 1 wherein said hardware security module is a security box attachable to said OPAL server computer.

47. An OPAL server computer as recited in claim 41 further comprising:

a memory arranged to store said virtual smart card database, said smart card emulator, and said pseudo card reader module.

48. An OPAL server computer as recited in claim 41 wherein said hardware security module is a hardware device in said OPAL server computer.

49. An OPAL server computer as recited in claim 41 wherein said hardware security module is a security box attachable to said OPAL server computer.

X. EVIDENCE APPENDIX

No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of 37 CFR, nor has any other evidence been entered by the examiner.

XI. RELATED PROCEEDINGS APPENDIX

There have been no decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 CFR 41.37(c)(1).